UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,877	08/14/2001	Yehuda Afek	0103376-00003	8704

21125 7590 07/17/2006

NUTTER MCCLENNEN & FISH LLP
WORLD TRADE CENTER WEST
155 SEAPORT BOULEVARD
BOSTON, MA 02210-2604

EXAMINER	
JEAN, FRANTZ B	

ART UNIT	PAPER NUMBER
2151	

DATE MAILED: 07/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/929,877	AFEK ET AL.	
	Examiner	Art Unit	
	Frantz B. Jean	2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,10,11,13-16,20,33,35 and 46-69* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,10,11,13-16,20,33,35,46-54 and 56-69* is/are rejected.

7)☒ Claim(s) *55* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/22/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This office action is in response to the amendment filed 03/20/2006. Claims 9, 12, 17-19, 21-32, 34, and 36-45 have been canceled. Claims 53-69 have been added. Accordingly, claims 1-8, 10-11, 13-16, 20, 33, 35, and 46-69 are pending in the application.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 12/22/05 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 103

Claims 1-8, 10-11, 13-16, 20, 33, 35, 46-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jungck US patent Number 6,829,654B1 in view of Davies US patent Number 6,901,053.

As per claim 1, Jungck teaches a method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims on a network [see col. 26 lines 29-55], the method comprising the steps of A. with a first set of one or more network elements external to the set of one or more potential victims [see elements 602A, 602B, 604A, 604B, the network elements can be internal or external see col. 27 lines 4-33; the potential victims are 108, 110], to a second set of one or more network elements external to the set of one or more potential victims traffic [col. 26 lines 35-50; col. 27 lines 34-46; col. 28 lines 21-39; col. 28 line 47 to col. 29 line 10], B. the element(s) of the second set filtering traffic diverted in step A ("diverted traffic") and

selectively passing a portion thereof to the victim [col. 28 lines 40-46; col. 29 lines 22-64]. However, Jungck does not explicitly teach initiating diversion of traffic destined for a victim due to an indication of anomalous traffic condition. Davies is directed a priority routing service that is provided for a predetermined network user in a connectionless network such as an IP network, which includes teach initiating diversion of traffic destined for a victim due to an indication of anomalous traffic condition (col. 5 line 32 to col. 6 line 5). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davies traffic diversion features with Jungck's system to provide an improved method of operating a network to mitigate the effects of congestion points within the network for high priority traffic (Davies col 1 lines 40-47).

As per claim 2, Jungck teaches a method according to claim 1, wherein the initiating step includes effecting a path of traffic that differs from a path that traffic would otherwise take to the victim [redirecting; col. 32 lines 58-60; col. 28 lines 21-34].

As per claim 3, Jungck teaches a method according to claim 1, wherein the filtering step includes detecting any of (i) a traffic pattern that differs from an expected pattern and (ii) traffic volume that differ from expected volume, the detecting step includes determining whether any of the traffic pattern and volume varies statistically significantly [DDOS attack; col. 28 line 40 to col. 29 line10].

As per claim 4, Jungck teaches a method according to claim 1, wherein the filtering step

includes detecting suspected malicious traffic [malicious program code, viruses and so on ... col. 28 lines 51 et seq].

As per claim 5, Jungck teaches a method according to claim 4, wherein the detecting step includes detecting packets with spoofed source addresses (col. 26 lines 29-50; col. 28 lines 51 et seq].

As per claim 6, Jungck teaches a method according to claim 1, wherein the filtering step includes detecting traffic requiring a selected service from the victim [col. 29 lines 22-64].

As per claim 7, Jungck teaches a method according to claim 6, wherein the filtering step includes discarding traffic not requiring the selected service from the victim [col. 29 lines 22-64].

As per claim 8, Jungck teaches a method according to claim 7, wherein the filtering step includes discarding any of UDP (is a connectionless mode protocol) and ICMP (is an integral part of IP) packet traffic [col. 28 lines 40-46; col. 31 lines 1-20].

As per claim 10, Jungck teaches a method according to claim 1, comprising operating one or more elements of the first set at points on the network around the set of one or more potential victim [col. 27 line 34 to col. 28 line 39].

As per claim 11, Jungck teaches a method according to claim 10, comprising operating one or more elements of the second set any of adjacent to or external to one or more elements of the first set [col. 27 line 34 to col. 28 line 39].

As per claim 13, Jungck teaches a method according to claim 10, detecting a distributed denial of service (DDoS) attack, or receiving a notification thereof [col. 28 lines 47 et seq].

As per claim 14, Jungck teaches a method according to claim 10, comprising selectively activating the one or more elements of the first set declaring a network address of the victim to be close in network distance to one or more elements of the second set [col. 13 lines 1-19; col. 15 lines 7-37; col. 20 line 65 to col. 21 line 11].

As per claim Jungck teaches 15, a method according to claim 10, comprising associating victim with first and second addresses, and wherein the filtering step includes discarding traffic received external to an area defined by the points directed to the first address, and passing traffic to the victim traffic received external to an area directed to the second address [col. 27 lines 34-51; col 28 lines 21-39].

As per claim 16, Jungck teaches a method according to claim 10, wherein the diverting steps includes redirecting traffic using Policy Based Routing [col. 27 line 13].

As per claim 20, Jungck teaches a method according to claim 5, which includes executing a verification protocol with sources of the diverted traffic [once traffic is intercepted, verification is performed to determine certain criteria related to the data and its destination; col. 28 lines 47 et seq], and wherein the passing step includes passing to the victim traffic from a source that correctly complies with the verification protocol [col. 18 lines 28-67; col. 27 lines 4 et seq].

As per claim 33, Jungck teaches a method according to claim 1, wherein the filtering step includes statistically measuring [investigating] any of the traffic pattern and volume so as to identify any of a source and a type of the overload condition [col. 28 line 47 to col. 29 line 10], [see also, Davies col 5 line 32 to col. 6 line 5].

As per claim 35, Jungck teaches a method according to claim 33, comprising determining any of the traffic pattern and volume during a period when the victim is not in the overload condition, for comparison with any of the traffic pattern and volume in the filtering step upon detecting ... [col. 29 lines 22-64].

As per claim 46, Jungck teaches a network element [602] for use in protecting against an overload condition on a network, the network element comprising: an input for receiving traffic diverted from the network [col. 27 lines 34-46; and 9-19], the traffic comprising flows of data packets having respective source addresses; a filter (606),

which is operative responsively to detection of the anomalous pattern, to block at least a portion of the data packets having the at least one of the source addresses; and an output coupled to the input for selectively passing on to further elements in the network traffic not blocked by the filter [col. 29 lines 22-64; col. 28 line 40 to col. 29 line 10]. Jungck does not explicitly detail on a statistics module that is arranged to perform a statistical analysis of the diverted traffic so as to detect an anomalous pattern of a flow associated with at least one of the source addresses. Davies teaches the above features (see Davies fig 3). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davies traffic diversion features with Jungck's system to provide an improved method of operating a network to mitigate the effects of congestion points within the network for high priority traffic (Davies col 1 lines 40-47).

As per claim 47, Jungck teaches a network element according to claim 46, comprising a termination detection module that at least participates in determining when the overload condition has ended [col. 28 line 47 to col. 29 line 10].

As per claim 48, Jungck teaches a network element according to claim 46, comprising an antispoofing element that performs at least one of the authenticating and verifying a source of traffic [col. 28 line 47 to col 29 line 64].

As per claim 49, Jungck teaches a system for use in protecting against an overload condition on a network, the system comprising: one or more network elements

("guards") [602A, 602B] disposed on the network, each network element having an input for receiving traffic from the network, a filter [606] coupled to the input, the filter selectively blocking traffic originating from a source suspected as potentially causing the overload condition, a statistics module that is coupled to the filter and that identifies the traffic statistically indicative of having originated from a source suspected as potentially causing the overload condition [col. 27 lines 4-46; col. 29 lines 22-64], and an output coupled to the input for selectively passing on to further elements in the network traffic not blocked by the filter, one or more further network elements ("diverters") disposed on the network and in communication with the guards, the further network elements ... guards traffic otherwise destined for a still further network element ("victim") in a set of one or more potential victims on the network [col. 27 lines 4-46; col. 29 lines 22-64]. However, Jungck does not explicitly teach initiating diversion of traffic destined for a victim due to an indication of anomalous traffic condition. Davies is directed a priority routing service that is provided for a predetermined network user in a connectionless network such as an IP network, which includes teach initiating diversion of traffic destined for a victim due to an indication of anomalous traffic condition (col. 5 line 32 to col. 6 line 5). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davies traffic diversion features with Jungck's system to provide an improved method of operating a network to mitigate the effects of congestion points within the network for high priority traffic (Davies col 1 lines 40-47).

As per claim 50, Jungck teaches a system according to claim 49, wherein at least one

of the guards comprises a termination detection module that at least participates in determining when the overload condition has ended [col. 28 line 47 to col. 29 line 10].

As per claim 51, Jungck teaches a system according to claim 49, wherein at least one of the guards comprises an ingress filter, coupled to the statistical module, that generates and transmits to a further network element on the network rules for blocking traffic on the network [col. 29 lines 11-64].

As per claim 52, Jungck teaches a system according to claim 49, comprising an antispoofing element that any of authenticates and verifies a source of traffic [col. 28 line 47 to col 29 line 64].

Claims 53-54 and 56-69 are new claims, which contain the same language of the claims already discussed above. Therefore, they are rejected under the same rationale.

Allowable Subject Matter

Claim 55 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Frantz B. Jean whose telephone number is 571-272-3937. The examiner can normally be reached on 8:30-6:00 M-f.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zarni Maung can be reached on 571 272 3939. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Frantz Jean

FRANTZ B. JEAN
PRIMARY EXAMINER